REMARKS

The following is intended as a full and complete response to the Final Office Action dated January 9, 2009, having a shortened statutory period for response set to expire on April 9, 2009. Claims 1-11 were examined. The Examiner rejected claims 1-11 under 35 USC § 103(a) as being unpatentable over Kim (US 6,584,199) in view of Albanese (US 2005/0033964). Applicants respectfully request reconsideration and withdrawal of these rejections for the reasons discussed below.

Rejections under 35 U.S.C. § 103(a)

Claim 1 recites the limitation of "including further management information in at least part of a first decryption messages (ECM's)." Claim 1 further recites the limitations of "testing whether the first decryption message (ECM) contains further management information targeted at a stream receiving device" ... and "indefinitely disabling subsequent decryption of at least part of the stream in the stream receiving device upon said detection." The Office Action concedes that Kim does not explicitly teach these limitations[1] but asserts that they are disclosed by Albanese.

Albanese discloses a communication process for establishing secure transmissions between a decoder and a smart card. The communication process begins with the decoder generating a session number S and a random number A1, encrypting these numbers using the smart card's public key, and sending the encrypted session number S and the random number A1 to the smart card (see paragraph [0006] of Albanese). In the smart card, numbers S and A1 are decrypted using the smart card's private key. The smart card then generates a second random number A2, encodes this random number and the session number S using the decoder's public key, and sends the encrypted session number S and the random number A2 to the decoder (see paragraph [0007] of Albanese). The decoder, in turn, decrypts numbers S and A2 using the decoder's private key and checks whether the decrypted number S is indeed the one initially sent by the decoder. If this is not the case, the communication process is stopped. Otherwise, a random session key K is generated in the decoder by means of a chopping function and values S,

[1] Final Office Action, page 5, lines 19-24.

A1, and A2. The decoder then uses the key K to encrypt S and sends S encrypted with the key K to the smart card (see paragraph [0008] of Albanese). In the smart card, S is decrypted by means of K and a check is made whether the decrypted number S is indeed the initial number sent. If this is not the case, the communication process between the decoder and the smart card is stopped.

Albanese teaches that the communication process described above constitutes the opening of a communication session between the decoder and the smart card (see paragraph [0054] of Albanese). Following the opening of the session, the decoder can send to the smart card entitlement control messages (ECMs) encrypted using the key K and the smart card can send to the decoder the control words also encrypted using the key K, thereby making the data exchange between the decoder and the smart card more secure (see paragraphs [0054], [0055], and [0051] of Albanese).

Applicants respectfully submit that the Examiner misinterpreted Albanese in concluding that paragraphs [0022]-[0031] and [0040]-[0041] of Albanese disclose "including further management information in at least part of the first decryption messages (ECM's)"... "testing whether the first decryption message (ECM) contains further management information targeted at a stream receiving device," and "indefinitely disabling subsequent decryption of at least part of the stream in the stream receiving device upon said detection." The paragraphs cited from Albanese merely recap the communication process described above, which is a process that takes place before any of the ECMs are sent. Neither the cited paragraphs nor any other paragraphs of Albanese teach including further management information as a part of the ECMs, as recited in claim 1.

As explained in paragraph [0007] of the present application, including further information in a part of some ECMs makes these ECMs "poisonous" for the selected stream receivers, thereby indefinitely disabling supply of control words. Since, on one hand, hackers need to supply ECMs to a secure device to profit from the stream, but, on the other hand, cannot determine beforehand which ECMs are poisonous for their secure device, including further information into the ECMs defeats the attempts of hackers to get illegal access.

As the foregoing illustrates, the steps of including further management information in at least part of a first decryption messages (ECM's), testing whether the first decryption message (ECM) contains further management information targeted at a stream receiving device, and indefinitely disabling subsequent decryption of at least part of the stream in the stream receiving device upon said detection is not disclosed in Albanese, contrary to the Examiner's assertion that it is.

By the Examiner's own admission, that which is not disclosed in Albanese is not taught in Kim. Therefore, the Office Action's proposed combination of the cited references fails to make a prima facie showing of obviousness of claim 1 over Kin in view of Albanese. For this reason, Applicant submits that claim 1 is in condition for allowance and requests that the 103 rejection be withdrawn.

Furthermore, claims 4, 7, 10, and 11 recite limitations similar to those of claim 1. Therefore, these claims are in condition for allowance for at least the same reasons as claim 1. Claims 2, 3, 5, 6, 8, and 9 are dependent from allowable claims 1, 4, and 7 and, therefore, are also in condition for allowance.

CONCLUSION

Based on the above remarks, Applicants believe that they have overcome all of the rejections set forth in the Final Office Action dated January 9, 2009, having a shortened statutory period for response set to expire on April 9, 2009, and that the pending claims are in condition for allowance. If the Examiner has any questions, please contact the Applicant's undersigned representative at the number provided below.

If necessary, please charge any additional fees or deficiencies, or credit any overpayments to Deposit Account No. 19-0743.

Respectfully submitted,

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(612) 373-6970

Date March 5, 2009

By
Charles E. Steffey
Reg. No. 25,179

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being filed using the USPTO's electronic filing system EFS-Web, and is addressed to: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on March 5, 2009.

CHERYL L. DANKERS
Name

Signature